

IN THE CLAIMS

1. [Currently amended] Method carried out on a computer for managing certificates in a certificate authority in a system having at least a first plurality of certificate authorities, comprising at least the steps of

[generating] using a computer to generate [at least two certificate revocation lists] a first certificate revocation list of a first type and having a first validity period,

using a computer to generate a second certificate revocation list of a first type wherein said second certificate revocation list has a validity period which is at least partially consecutive with said first validity period and which has a beginning time which is a future point in time; and

each of said [at least two] first and second certificate revocation lists of a first type listing one or more certificate authorities, and not indicating a revoked status of any said certificate authority in said at least a first plurality of certificate authorities[.].

[said at least two certificate revocation lists of a first type having at least partially consecutive validity period,

where the beginning of the validity period of at least one of said at least two certificate revocation lists of a first type is a future point of time.]

2. [Currently amended] Method according to claim 1, comprising at least the steps of

publishing at least said first and second certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

3. [Currently amended] Method according to claim 1, comprising at least the steps of

checking regarding each of said certificate authorities listed in said certification revocation lists of a first type if the security of each of said certificate authorities has been breached or not;

and if the security of none of said certificate authorities has been breached, publishing one of said certificate revocation lists of a first type having the appropriate validity period for the time of publication.

4. [Currently amended] Method according to claim 1, further comprising at least the steps of

[generating] using a computer to generate at least [two] first and second certificate revocationlists (CRLs) of a second type,

each of said at least [two] first and second certificate revocation lists of a second type indicating a revoked status of at least one said certificate authority in said at least a first plurality of certificate authorities,

said [at least two] first and second certificate revocation lists of a second type having at least partially consecutive validity periods,

and wherein [where] the beginning of the validity period of said [at least one of said at least two] second certificate revocation [lists] list of a second type is a future point of time.

5. [Currently amended] Method according to claim 4, further comprising at least the steps of

checking regarding each of said certificate authorities in said at least a first

plurality of certificate authorities if the security of each of said certificate authorities has been breached or not;

and if the security of none of said certificate authorities has been breached,
5 publishing [one of] said first of said first and second certificate revocation lists of a first type,

and if the security of at least one of said certificate authorities has been breached
10 after publication of said first of said first and second certificate revocation lists of said first type, publishing at least one of said certificate revocation lists of a second type.

6. [Currently amended] Method according to claim 4, further comprising at least
15 the steps of

[generating] using a computer to generate for each certificate authority in said at least a first plurality of certificate authorities, if the security of [each of] a certificate authority has been breached, at least one certificate revocation list of a
20 second type in a series of certificate revocation lists of said second type which indicates a revoked status of said certificate authority.

7. [Currently amended] Method according to claim 1, comprising at least the
25 steps of

[generating] using a computer to generate at least [two] first and second certificate revocation lists of a third type,

30 each of said at least [two] first and second certificate revocation lists of a third type indicating a temporarily suspended status of at least one certificate authority in said at least a first plurality of certificate authorities,

said at least [two] first and second certificate revocation lists of a third type having at least partially consecutive validity periods,

5 where the beginning of the validity period of at least one of said [at least two certificate revocation lists] first and second revocation lists of a third type is a future point of time.

10 8. [Currently amended] [System] An apparatus for managing certificate revocation lists for a certificate authority having [means for generating certificate revocation lists,] comprising at least::

a computer programmed with an operating system and one or more programs which cooperate with said operating system to control said computer to perform the following process:

15 [means for] generating sequences of certificate revocation lists of a first type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a first type being a future point of time relative to the time of generating a sequence of certificate revocation lists,

20 and wherein said certificate revocation lists of [a] said first type indicating no revocation for a predefined group of certificate authorities.

25 9. [Currently amended] [System] An apparatus according to claim 8, [future] wherein said one or more programs further comprise program code which controls said computer to publish [comprising at least means for publishing] said certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

10. [Currently amended] [System] An apparatus according to claim 8,
[comprising at least] wherein said one or more programs further comprise
program code which controls said computer to perform the following additional
steps:

5 [means for] generating sequences of certificate revocation lists of a
second type having at least partially consecutive validity periods, the beginning of
the validity period of at least one of said revocation lists of a second type being a
future point of time relative to the time of generating a sequence of certificate
revocation lists, and

10 [means for] generating an indication of revoked status of at least one
certificate authority in said predefined group of certificate authorities in each
certificate revocation list generated by said means for generating sequences of
certificate revocation lists of a second type.

15

11. [Currently amended] [System] An apparatus according to claim 10,
[comprising at least] wherein said one or more programs further comprise
program code which controls said computer to perform the following additional
steps:

20 [means for] checking regarding each of certificate authorities in said
predefined group of certificate authorities if the security of each of said certificate
authorities has been breached or not:

 [means for] publishing one of said certificate revocation lists of [a] said
first type if the security of none of said certificate authorities has been breached,
25 and

 [means for] publishing one of said certificate revocation lists of [a] said
second type if the security of at least one of said certificate authorities has been
breached.

30

12. [Currently amended] [Computer program product for a certificate authority having computer code means for generating] A computer-readable medium having stored thereon computer program code for controlling a computer to generate certificate revocation lists using the following process, comprising at least

[computer program code means for] generating sequences of certificate revocation lists of a first type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a first type being a future point of time relative to the time of generating a sequence of certificate revocation lists,

said certificate revocation lists of a first type indicating no revocation for a predefined group of certificate authorities.

13. [Currently amended] [Computer program product according to] The computer-readable medium as defined in claim 12, wherein said computer program code further comprises computer program code for controlling said computer to publish [comprising at least computer program code means for publishing] said certificate revocation lists of a first type one at a time, each essentially at the time of the beginning of the validity period of that particular certificate revocation list.

14. [Currently amended] [Computer program product according to] The computer-readable medium as defined in claim 12, wherein said computer program code stored on said medium further comprises code for controlling said computer to perform the following additional process steps: [comprising at least]

[computer program code means for generating] generating in advance a sequence [sequences] of certificate revocation lists of a second type having at least partially consecutive validity periods, the beginning of the validity period of

at least one of said revocation lists of a second type being a future point of time relative to the time of generating a sequence of certificate revocation lists, and

[computer program code means for generating] generating an indication of revoked status of at least one certificate authority in said predefined group of certificate authorities in each of said_certificate revocation lists of said second type generated in advance [by said means for generating sequences of certificate revocation lists of a second type].

15. [Currently amended] [Computer program product according to] A computer readable medium as defined in claim 14, [comprising at least] wherein said computer program code stored on said medium further comprises code for controlling said computer to perform the following additional process steps:

[computer program code means for] checking for security breaches regarding each of said certificate authorities in said predefined group of certificate authorities; [if the security of each of said certificate authorities has been breached or not;]

[program code means for] publishing one of said certificate revocation lists of a first type if the security of none of said certificate authorities has been breached, and

[computer program code means for] publishing one of said certificate revocation lists of a second type if the security of at least one of said certificate authorities has been breached.

16. [New] A process carried out on a computer for managing root certificates revocation lists (root CRLs) for sub-Certificate Authorities (sub-CAs) in a certificate authority comprising at least the steps of:

A) using a computer to generate in advance a plurality of certificate revocation lists CRL) of a first type having partially consecutive validity periods which may have overlap in time of coverage of said validity periods but the sequence of validity periods of

said CRLs of said first type have no gaps in time, the beginning in time of the validity period of each CRL of said first type after a first of said CRLs of said first type being a future point in time, and wherein none of said CRLs of said first type indicate revoked status for any sub-CA;

- 5 B) using a computer to generate in advance for each sub-CA a sequence of CRLs of a second type having partially consecutive validity periods which may have overlap in time of coverage of said validity periods but the sequence of validity periods of said CRLs of said second type having no gaps in time, the beginning in time of the validity period of each CRL of said second type after a first of said CRLs of said second
- 10 type being a future point in time, and wherein each of said CRLs of said second type indicate revoked status for the particular sub-CA to which said second CRL of said second type pertains;

(C) repeating step B for each sub-CA so as to generate in advance a separate sequence of CRLs of said second type for each sub-CA;

- 15 (D) as the beginning of the validity period of each said CRL of said first type approaches, checking to determine if the security of any sub-CA has been breached, and, if not, publishing a CRL of said first type, and, if the security of a sub-CA has been breached, selecting a CRL of said second type indicating revoked status for said sub-CA whose security has been breached and having an appropriate validity period and
- 20 publishing said selected CRL of said second type.

17. [New] The process of claim 16 further comprising the step of storing at least one of said CRLs of said first and second type in an on-line system.

- 25 18. The process of claim 17 further comprising the step of storing at least one of said CRLs of said first and second type in a plaintext form.

19. The process of claim 17 further comprising the step of storing at least one of said CRLs of said first and second type in encrypted form.

30

20. The process of claim 19 further comprising the step of encrypting said at least one of said CRLs of the first and second type with a secret, said secret being either a secret stored in memory or a secret entered by an operator.

- 5 21. [New] A process carried out on a computer for managing root certificates revocation lists (root CRLs) for sub-Certificate Authorities (sub-CAs) in a certificate authority comprising at least the steps of:

A) using a computer to generate in advance a plurality of certificate revocation lists CRL) of a first type having partially consecutive validity periods which may have
10 overlap in time of coverage of said validity periods but the sequence of validity periods of said CRLs of said first type have no gaps in time, the beginning in time of the validity period of each CRL of said first type after a first of said CRLs of said first type being a future point in time, and wherein none of said CRLs of said first type indicate revoked status for any sub-CA;

15 (B) as the beginning of the validity period of each said CRL of said first type approaches, checking to determine if the security of any sub-CA has been breached, and, if not, publishing a CRL of said first type, and, if the security of a sub-CA has been breached, discarding the CRL of said first type with the beginning of the validity period which is approaching and using a computer to generate and publish a new CRL of a
20 second type indicating at least revoked status for said sub-CA whose security has been breached, said CRL of said second type generated in this step having a validity period which is partially consecutive with the validity period of said CRL of said first type such that there is no gap in time between the end of the validity period of said CRL of said first type and the validity period of said CRL of said second type generated in this step B.

25

22. [new] The process of claim 21 further comprising the step of storing at least one of said CRLs in an on-line system.

23. The process of claim 22 further comprising the step of storing at least one of said
30 CRLs of said first and second type in a plaintext form.

24. The process of claim 22 further comprising the step of storing at least one of said CRLs of said first and second type in encrypted form.

25. The process of claim 24 further comprising the step of encrypting said at least one of said CRLs of the first and second type with a secret, said secret being either a secret stored in memory or a secret entered by an operator.

5

26. [New] A process carried out on a computer for managing root certificates revocation lists (root CRLs) for sub-Certificate Authorities (sub-CAs) in a certificate authority comprising at least the steps of:

10 A) using a computer to generate in advance a plurality of certificate revocation lists CRL) of a first type having partially consecutive validity periods which may have overlap in time of coverage of said validity periods but the sequence of validity periods of said CRLs of said first type have no gaps in time, the beginning in time of the validity period of each CRL of said first type after a first of said CRLs of said first type being a future point in time, and wherein none of said CRLs of said first type indicate revoked
15 status for any sub-CA;

 B) using a computer to generate in advance for each possible subcombinations of sub-CA a sequence of CRLs of a second type, each sequence having partially consecutive validity periods which may have overlap in time of coverage of said validity periods but the sequence of validity periods of said CRLs of said second type having no
20 gaps in time, the beginning in time of the validity period of each CRL of said second type after a first of said CRLs of said second type being a future point in time, and wherein each of said CRLs of said second type in each said sequence of CRLs of said second type indicating revoked status for one subcombinations of sub-CAs;

 (C) as the beginning of the validity period of each said CRL of said first type
25 approaches, checking to determine if the security of any sub-CA or sub-combination of sub-CAs has been breached, and, if not, publishing a CRL of said first type, and, if the security of any sub-CA or subcombination of sub-CAs has been breached, selecting a CRL of said second type indicating revoked status for said sub-CA or sub-combination of sub-CAs whose security has been breached and having an appropriate validity period
30 and publishing said selected CRL of said second type.

27. [new] The process of claim 26 further comprising the step of storing at least one of said CRLs in an on-line system.

28. The process of claim 27 further comprising the step of storing at least one of said
5 CRLs of said first and second type in a plaintext form.

29. The process of claim 27 further comprising the step of storing at least one of said CRLs of said first and second type in encrypted form.

10 30. The process of claim 29 further comprising the step of encrypting said at least one of said CRLs of the first and second type with a secret, said secret being either a secret stored in memory or a secret entered by an operator.

15 31. [New] System for a certificate authority having means for generating certificate revocation lists, comprising at least

means for generating sequences of certificate revocation lists of a first type having at least partially consecutive validity periods, the beginning of the validity period of at least one of said revocation lists of a first type being a future point of time relative to the time of generating a sequence of certificate
20 revocation lists,

means for generating sequences of certificate revocation lists of a second type and a third type, each sequence having at least partially consecutive validity periods;

25 said certificate revocation lists of a first type indicating no revocation for a predefined group of certificate authorities, and said certificate revocation lists of said second type indicating a revoked status for one or more certificate authorities, and said certificate revocation lists of said third type indicating a temporarily suspended status of a certificate authority; and

30 means for checking for security breaches of said certificate authorities before the beginning of the validity period of each certificate revocation list in said sequence of certificate revocation lists of said first type, and if no security breach has occurred publishing a certificate revocation list of a first type, and if a security

5 breach has definitely occurred, selecting a certificate revocation list of a second type having an appropriate validity period and publishing it, and if it is not clear whether a security breach for one or more certificate authorities has occurred, selecting and publishing a certificate revocation list of a third type having an appropriate validity period and indicating a temporarily suspended status for the one or more certificate authorities whose security might have been breached.